SONICWALL GLOBAL VPN CLIENT 2.0

USER'S GUIDE

SONICWALL

Table of Contents

Introduction 1
SonicWALL Global VPN Client Features 1

About this Guide 3
Conventions Used in this Guide 3
Icons Used in this Guide 3

Copyright Notice 4

Installing the SonicWALL Global VPN Client 5
Using the Setup Wizard 5

Adding VPN Connection Policies 8
VPN Connection Policies 9
Digital Certificates 9
Using the New Connection Wizard 10
Creating a VPN Connection Policy 10
Importing a VPN Configuration File 12

Launching the SonicWALL Global VPN Client 13

Making VPN Connections 15
Enabling a VPN Connection 16
Establishing Multiple Connections 16
Entering a Pre-Shared Key 17
Username and Password Authentication 18
Connection Warning 18

Disabling a VPN Connection 19

Checking the Status of a VPN Connection 19

Creating a VPN Policy Shortcut 20

Specifying Global VPN Client Launch Options 21

SonicWALL Global VPN Client System Tray Icon 22

Managing VPN Connection Policy Properties 22
General 23
Windows NT/2000 Authentication via Logon Script 24
User Authentication 25
Peers 26
Peer Information Dialog Box 27
Status 29

Managing VPN Connection Policies 31
Displaying Connection Policies 31
Arranging Connection Policies 31
Renaming a Connection Policy 31
Deleting a Connection Policy 31
Selecting All Connection Policies 31

Managing Certificates 32

Troubleshooting SonicWALL Global VPN Client 33
Log Viewer 33
Setting Up Log Files 35
Generating a Help Report 36
Technical Support 37
Help Topics 37
Uninstalling the SonicWALL Global VPN Client 37

SONICWALL GLOBAL VPN CLIENT SOFTWARE LICENSE AGREEMENT 38
LICENSE 39
EXPORTS LICENSE 39
SUPPORT SERVICES 39
UPGRADES 39
COPYRIGHT 40
U.S. GOVERNMENT RESTRICTED RIGHTS 40
MISCELLANEOUS 40
TERMINATION 40
LIMITED WARRANTY 41
CUSTOMER REMEDIES 41
NO OTHER WARRANTIES 41
LIMITATION OF LIABILITY 41

SonicWALL Global VPN Client Support 42

Appendix A: Using the default.rcf File 43

How the Global VPN Client uses the default.rcf File 44
Installing the default.rcf File 44
Include the default.rcf File with the Global VPN Client Software 44
Add the default.rcf file to the Default Global VPN Client Directory 45
Replace the Existing SonicWALL Global VPN Client.rcf File 45
Troubleshooting 45

Appendix B - Running the Global VPN Client from the Command Line 46

Introduction

The SonicWALL Global VPN Client creates a Virtual Private Network (VPN) connection between your computer and the corporate network to maintain the confidentiality of private data. The Global VPN Client provides an easy-to-use solution for secure, encrypted access through the Internet or corporate dial-up facilities for remote users such as mobile employees or telecommuters. The Global VPN Client also provides secure wireless networking for SonicWALL SOHO TZW clients using SonicWALL's WiFiSec technology.

Custom developed by SonicWALL, the Global VPN Client combines with GroupVPN on SonicWALL Internet Security Appliances to dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, the SonicWALL administrators establishes the VPN connections policies for the Global VPN Clients. The VPN configuration data is transparently downloaded from the SonicWALL VPN Gateway (SonicWALL Internet Security Appliance) to Global VPN Clients, removing the burden of provisioning VPN connections from the user.

SonicWALL Global VPN Client Features

The SonicWALL Global VPN Client delivers a robust IPSec VPN solution with these features:

- **Easy to Use** - Provides an easy-to-follow Installation Wizard to quickly install the product, an easy-to-follow Configuration Wizard with common VPN deployment scenarios, point-and-click activation of VPN connections, and streamlined management tools to minimize support requirements.
- **Client Policy Provisioning** - Using only the IP address or Fully Qualified Domain Name (FQDN) of the SonicWALL VPN gateway, the VPN configuration data is automatically downloaded from the SonicWALL VPN gateway via a secure IPSec tunnel, removing the burden from the remote user of provisioning VPN connections.
- **XAUTH Authentication with RADIUS** - Provides added security with user authentication after the client has been authenticated via a RADIUS server.
- **VPN Session Reliability** - Allows automatic redirect in case of a SonicWALL VPN gateway failure. If a SonicWALL VPN gateway is down then the Global VPN Client can go through another SonicWALL VPN gateway.
- **Multiple Subnet Support** - Allows Global VPN Client connections to more than one subnet in the configuration to increase networking flexibility.
- **Third-Party Certificate Support** - Supports VeriSign, Entrust, Microsoft, and Netscape Certificate Authorities (CAs) for enhanced user authentication.
- **Tunnel All Support** - Provides enhanced security by blocking all traffic not directed to the VPN tunnel to prevent Internet attacks from entering the corporate network through a VPN connection.
- **DHCP over VPN Support** - Allows IP address provisioning across a VPN tunnel for the corporate network while allowing WAN DHCP for Internet Access from the ISP.
- **Secure VPN Configuration** - Critical Global VPN Client configuration information is locked from the user to prevent tampering.

- **AES and 3DES Encryption** - Supports 168-bit key 3DES (Data Encryption Standard) and the new U.S. Government encryption standard AES (Advanced Encryption Standard) for dramatically increased security. AES requires SonicOS 2.0.
- **GMS Management** - Allows Global VPN Client connections to be managed by SonicWALL's award-winning Global Management System (GMS).
- **Multi-Platform Client Support** - Supports Windows 98 SE, Windows ME, Windows NT 4.0 (service pack 6 or later), Windows 2000 Professional (service pack 3 or later), Windows XP Professional, Windows XP Home Edition, and Windows XP Tablet PC Edition.
- **NAT Traversal -** Enables Global VPN Client connections to be initiated from behind any device performing NAT (Network Address Translation). The SonicWALL Global VPN Client encapsulates IPSec VPN traffic to pass through NAT devices, which are widely deployed to allow local networks to use one external IP address for an entire network.
- **Automatic Reconnect When Error Occurs** - Allows the Global VPN Client to keep retrying a connection if it encounters a problem connecting to a peer. This feature allows the Global VPN Client to automatically make a connection to a SonicWALL VPN gateway that is temporarily disabled, without manual intervention.
- **Ghost Installation for Large Scale Installations** - Enables the Global VPN Client's virtual adapter to get its default address after installation and then create a ghost image.
- **NT Domain Logon Script Support** - Allows Global VPN Clients to perform Windows NT/ 2000 domain authentication after establishing a secure IPSec tunnel. The SonicWALL VPN gateway passes the logon script as part of the Global VPN Client configuration. This feature allows the VPN user to have access to mapped network drives and other network services.
- **Dual Processor Support** - Enables the Global VPN Client to operate on dual-processor computers.
- **Group Policy Management** - Global VPN Clients access can be customized and restricted to specific subnet access (Requires SonicOS 2.0).
- **Hub and Spoke VPN Access** - Allows IP addressing from SonicWALL VPN Gateway's DHCP Server to Global VPN Client for configuring a different subnet for all remote Global VPN Clients than the subnet of the LAN. Makes hub-and-spoke VPN access simpler. When a Global VPN Client successfully authenticates with the central site, it receives a virtual IP address that also grants it access to other trusted VPN sites.
- **Default VPN Connections File** - Enables the SonicWALL administrator to configure and distribute the corporate VPN connections with the Global VPN Client software to streamline VPN client
deployment.
- **Integration with Dial-Up Adapter** - Allows Global VPN Client connections using Microsoft Dial-Up Networking or third-party dial-up applications either as an automatic backup to a broadband connection or as the primary connection.
- **Single VPN Connection to any SOHO TZW for Roaming** - Allows users to use a single VPN connection policy to access multiple SOHO TZW wireless networks.

About this Guide

The *SonicWALL Global VPN Client User's Guide* provides complete documentation on installing, configuring, and managing the SonicWALL Global VPN Client. This guide is updated and released with Global VPN Client 2.0.0.0.

For complete documentation on configuring and managing SonicWALL Global VPN Clients and SonicWALL GroupVPN on the SonicWALL VPN Gateway, see the *SonicWALL Global VPN Client Administrator's Guide*.

Always check www.sonciwall.com/support/documentation.html for the latest version of this manual and other upgrade manuals as well.

Conventions Used in this Guide

Conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the Global VPN Client interface or the SonicWALL Management Interface.
Italic	Highlights a value to enter into a field. For example, "type *192.168.168.168* in the **IP Address** field."
>	Indicates a multiple step menu choice. For example, "select **File>Open**" means "select the **File** menu, then select the **Open** item from the **File** menu.

Icons Used in this Guide

Alert! *Important information about features that can affect performance, security features, or cause potential problems with your SonicWALL.*

Tip! *Useful information about security features and configurations on your SonicWALL.*

Note! *Related information to the topic*.

Copyright Notice

© 2003 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice. October 2003

Installing the SonicWALL Global VPN Client

The Global VPN Client uses an easy-to-use wizard to guide you through the installation process. The SonicWALL Global VPN Client supports Windows 98 SE, Windows ME, Windows NT 4.0 (service pack 6 or later), Windows 2000 Professional (service pack 3 or later), Windows XP Professional, Windows XP Home Edition, and Windows XP Tablet PC Edition.

Alert! *The SonicWALL Global VPN Client requires a SonicWALL gateway running firmware version 6.4.2.0 (or higher), SonicOS 1.0.0.0 (or higher) and a 3rd generation SonicWALL Internet Security Appliance or SonicOS Standard 2.0.0.0/SonicOS Enhanced 2.0.0.0 and a 4th generation SonicWALL Internet Security Appliance.*

Tip! *You can upgrade the SonicWALL Global VPN Client 1.0 to 2.0 without uninstalling 1.0.*

Using the Setup Wizard

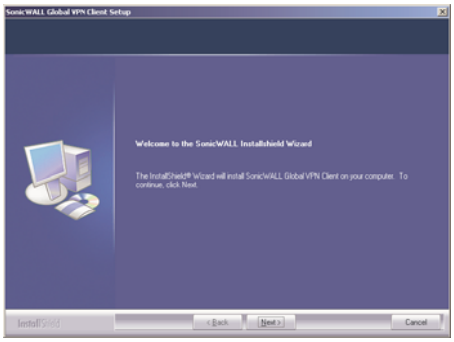
The following steps explain how to install the SonicWALL Global VPN Client program using the **Setup Wizard**. You use the **Setup Wizard** for a new Global VPN Client installation or upgrading a previous version of the SonicWALL Global VPN Client. If you're upgrading your Global VPN Client software, the **Setup Wizard** doesn't display all the same pages as a new installation.

Alert! *Remove any installed 3rd Party VPN client program before installing the SonicWALL Global VPN Client.*

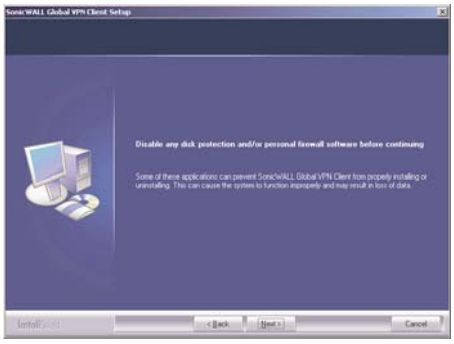
Alert! *Installing the Global VPN Client on Windows NT, Windows 2000, and Windows XP requires Administrator rights.*

Alert! *You must use a Zip program to unzip the SonicWALL Global VPN Client program files before installing it.*

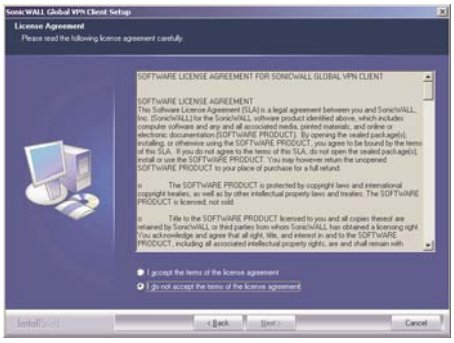
1. Unzip the SonicWALL Global VPN Client program.
2. Double-click **setup.exe**. The **Setup Wizard** launches.


SonicWALL Global VPN Client Setup
Welcome to the SonicWALL InstallShield Wizard
The InstallShield® Wizard will install SonicWALL Global VPN Client on your computer. To continue, click Next.
InstallShield
< Back
Next >
Cancel

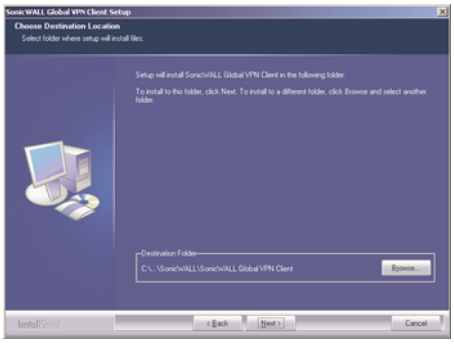
3. Click **Next** to continue installation of the VPN Client.


SonicWALL Global VPN Client Setup
Disable any disk protection and/or personal firewall software before continuing
Some of these applications can prevent SonicWALL Global VPN Client from properly installing or uninstalling. This can cause the system to function improperly and may result in loss of data.
InstallShield
< Back
Next >
Cancel

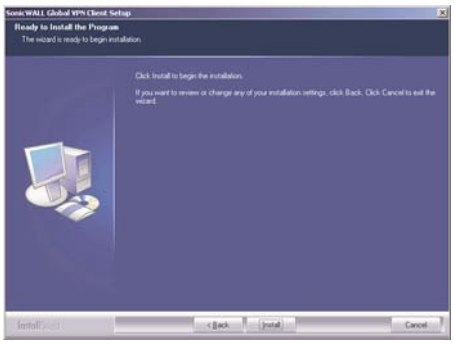
4. Close all applications and disable any disk protection and personal firewall software running on your computer. Click **Next**.


SonicWALL Global VPN Client Setup
License Agreement
Please read the following license agreement carefully.
SOFTWARE LICENSE AGREEMENT FOR SONICWALL GLOBAL VPN CLIENT
SOFTWARE LICENSE AGREEMENT
I accept the terms of the license agreement
I do not accept the terms of the license agreement
InstallShield
< Back
Next >
Cancel

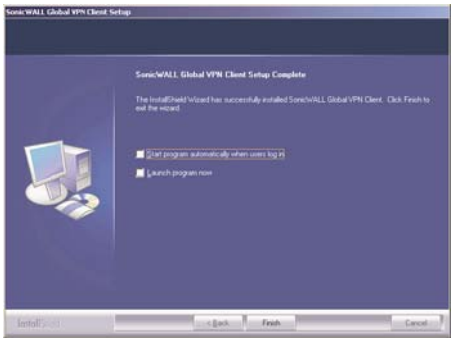
5. Select **I accept the terms of the license agreement**. Click **Next**.


SonicWALL Global VPN Client Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install SonicWALL Global VPN Client in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\SonicWALL\SonicWALL Global VPN Client
Browse...
InstallShield
< Back
Next >
Cancel

6. Click **Next** to accept the default location and continue installation or click **Browse** to specify a different location.


SonicWALL Global VPN Client Setup
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

7. Click **Install**. The **Setup Wizard** installs the Global VPN Client files on your computer. After the **Setup Wizard** installs the Global VPN Client, a dialog box is displayed asking you if you want to add the Global VPN Client to the Windows Quick Launch toolbar.
8. Click **Yes** to add the Global VPN Client to the Quick Launch toolbar or click **No**.


SonicWALL Global VPN Client Setup
SonicWALL Global VPN Client Setup Complete
The InstallShield Wizard has successfully installed SonicWALL Global VPN Client. Click Finish to exit the wizard.
Start program automatically when users log in
Launch program now
InstallShield
< Back
Finish
Cancel

9. Select **Start VPN Global Client Automatically when users log in** to automatically launch the VPN Global Client when you log onto the computer, if desired.
10. Select **Launch program now** to automatically launch the Global VPN Client after finishing the installation, if desired.
11. Click **Finish**.

Adding VPN Connection Policies

Adding a new VPN connection policy is easy because SonicWALL's Client Policy Provisioning automatically provides all the necessary configuration information to make a secure connection to the local or remote network. The burden of configuring the VPN connection parameters is removed from the Global VPN Client user. VPN connection policies can be created using three methods:

- Download the VPN policy from the SonicWALL VPN Gateway to the Global VPN Client using the **New Connection Wizard**. This wizard walks you through the process of locating the source of your configuration information and automatically downloads the VPN configuration information over a secure IPSec VPN tunnel. The **New Connection Wizard** provides easy configuration for the most common VPN scenarios. You choose the **Remote Access** configuration to create a VPN connection to a remote network from any broadband or dial-up connection over a wired or wireless network. You use the **Office Gateway** VPN connection policy to securely connect to SonicWALL SOHO TZW wireless networks.
- Import a VPN policy file into the SonicWALL Global VPN Client. The VPN policy is sent to you as a file, which you install using the **Import Connection** dialog box.
- Install the **default.rcf** file as part of the Global VPN Client software installation or add it after installing the Global VPN Client. If the SonicWALL VPN Gateway administrator included the **default.rcf** file as part of the Global VPN Client software, when the program is installed, one or more preconfigured VPN connections are automatically created.

Note! *Creating a **Default.rcf** file and distributing it with the Global VPN Client software allows you to quickly establish preconfigured VPN connections. When the Global VPN Client software is installed, the VPN policy created by the SonicWALL VPN Gateway administrator is automatically created. For more information on using the **Default.rcf** file, see "Appendix A: Using the default.rcf File" on page 43*

VPN Connection Policies

The Global VPN Client allows multiple connection policies to be configured at the same time, whether they are provisioned from multiple gateways or imported from one or more files. Because connection policies may be provisioned from multiple gateways, each connection policy explicitly states allowed behavior in the presence of any connection policy conflicts. You may have VPN connections that don't allow other VPN connections or Internet and network connections while the VPN policy is enabled.

The VPN connection policy includes all the parameters necessary to establish secure IPSec tunnels to the gateway. A connection policy includes Phase 1 and Phase 2 Security Associations (SA) parameters including:

- Encryption and authentication proposals
- Phase 1 identity payload type
- Phase 2 proxy IDs (traffic selectors)
- Client Phase 1 credential
- Allowed behavior of connection in presence of other active connections
- Client caching behavior

Digital Certificates

If digital certificates are required as part of your VPN connection policy, your gateway administrator must provide you with the required information to import the certificate. You then need to import the certificate in the Global VPN Client using the Certificate Manager.

Alert! *If digital certificates are required as part of your VPN connection policy, your VPN gateway administrator must provide you with the required certificates.*

Note! *For instructions on importing a certificate into the Global VPN Client, see* "Managing Certificates" on page 32

Using the New Connection Wizard

The **New Connection Wizard** allows you to configure your Global VPN Client for two VPN connection scenarios:

- **Remote Access** - You choose this scenario if you want secure access to a remote VPN gateway from any wired or wireless network. The most common use of this scenario is when you are at home or on the road and want access to the corporate network. You enter the IP address or FQDN (*gateway.yourcompany.com*) of the VPN gateway and the Global VPN Client automatically downloads the VPN connection policy from the remote SonicWALL VPN gateway.
- **Office Gateway** - You choose this scenario if you want secure access to a local SonicWALL SOHO TZW wireless network. When you create an **Office Gateway** VPN connection, it appears as the **Peer** entry of **<Default Gateway>** in the **SonicWALL Global VPN Client** window. You can use this single **Office Gateway** VPN connection policy to roam securely across SOHO TZW wireless networks.

Alert! *If you are configuring the Global VPN Client for **Remote Access**, make sure you have the IP address or FQDN (gateway.yourcompany.com) of the remote SonicWALL VPN gateway and an active Internet connection before using the **New Connection Wizard**.*

Alert! *If you are configuring the Global VPN Client for **Office Gateway**, make sure your wireless card is configured with the correct SSID information to access the SonicWALL SOHO TZW before using the **New Connection Wizard**.*

Creating a VPN Connection Policy

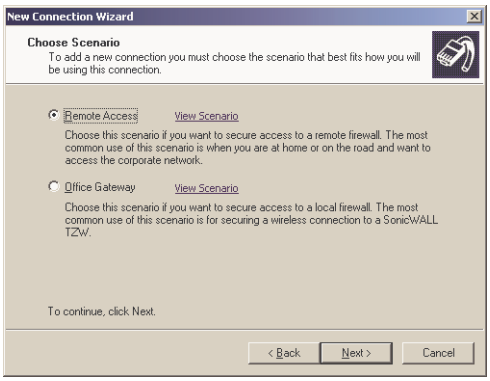
The following instructions explain how to use the **New Connection Wizard** to automatically download VPN connection policies for the Global VPN Client from a local or remote SonicWALL VPN gateway.

1. Choose **Start>Programs>SonicWALL Global VPN Client**. The first time you open the SonicWALL Global VPN Client, the **New Connection Wizard** automatically launches.

New Connection Wizard
Welcome to the New Connection Wizard
This wizard will guide you through the process of adding a new connection to your configuration.
SONICWALL
To continue, click Next.
< Back
Next >
Cancel

2. If the **New Connection Wizard** does not display, click the **New Connection Wizard** icon on the far left side of the toolbar to launch the **New Connection Wizard**. Click **Next**.

3. In the **Choose Scenario** page, select Remote Access or Office Gateway and then click **Next**. Click on **View Scenario** to view a diagram of each type of VPN connection.


New Connection Wizard
Choose Scenario
To add a new connection you must choose the scenario that best fits how you will be using this connection.
Remote Access
View Scenario
Choose this scenario if you want to secure access to a remote firewall. The most common use of this scenario is when you are at home or on the road and want to access the corporate network.
Office Gateway
View Scenario
Choose this scenario if you want to secure access to a local firewall. The most common use of this scenario is for securing a wireless connection to a SonicWALL TZW.
To continue, click Next.
< Back
Next >
Cancel

4. If you selected **Remote Access** in the **Choose Scenario page**, the **Remote Access** page is displayed. Type the IP address or FQDN of the gateway in the **IP Address or Domain Name** field. The information you type in the **IP Address or Domain Name** field appears in the **Connection Name** field. If you want a different name for your connection, type the new name for your VPN connection policy in the **Connection Name** field. Click **Next**.
5. In the **Completing the New Connection Wizard** page select any of the following options:

   Select **Enable this connection when the program is launched**, if you want to automatically establish this VPN connection when you launch the SonicWALL Global VPN Client.

   Select **Create a shortcut to this connection on the desktop**, if you want to create a shortcut icon on your desktop for this VPN connection.
6. Click **Finish.** The new VPN connection policy appears in the SonicWALL Global VPN Client window.

New Connection Wizard
Completing the Add Connection Wizard
You have successfully completed the Add Connection wizard. The connection will be added to your configuration.
Enable this connection when the program is launched
Create a shortcut to this connection on the desktop
To complete this wizard, click Finish.
SONICWALL
< Back
Finish
Cancel

Note! *You can change the default name by right-clicking the **Office Gateway** entry and selecting **Properties** from the menu. In the **General** tab of the **Properties** dialog box, enter the new name in the **Name** field.*

Importing a VPN Configuration File

A VPN connection policy can be created as a file and sent to you by the SonicWALL VPN gateway administrator. This VPN configuration file has the filename extension **.rcf**. If you received a VPN connection policy file from your administrator, you can install it using the **Import Connection** dialog box.

The VPN policy file is in the XML format to provide more efficient encoding of policy information. Because the file can be encrypted, pre-shared keys can also be exported in the file. The encryption method is specified in the PKCS#5 Password-Based Cryptography Standard from RSA Laboratories and uses Triple-DES encryption and SHA-1 message digest algorithms.

Alert! *If your **.rcf** file is encrypted, you must have the password to import the configuration file into the Global VPN Client.*

The following instructions explain how to add VPN connection policy by importing a connection policy file provided by your gateway administrator.

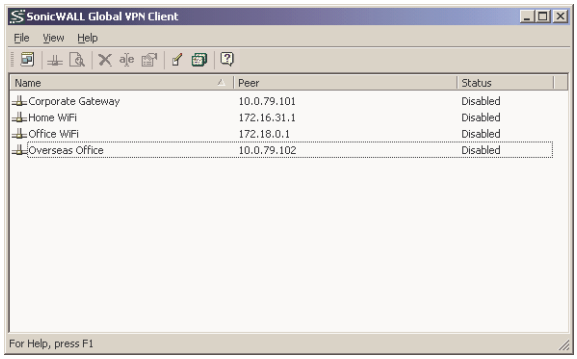
1. Choose **Start>Programs>SonicWALL Global VPN Client**.
2. Select **File>Import Connection**. The **Import Connection** dialog box is displayed.

Import Connection
This window allows you to import connection settings from a configuration file.
Specify the name of the configuration file to import:
If the file is encrypted, specify the password:
OK
Cancel

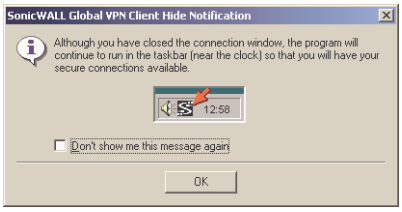
3. Type the file path for the configuration file in the **Specify the name of the configuration file to import** field or click the browse **...** button to locate the file. If the file is encrypted, enter the password in the **If the file is encrypted, specify the password** field.
4. Click **OK**.

Launching the SonicWALL Global VPN Client

To launch the SonicWALL Global VPN Client, choose **Start>Programs>SonicWALL Global VPN Client**.



The default setting for the SonicWALL Global VPN Client window is **Hide the window (reopen it from the tray icon)**. If you click **Close,** press **Alt+F4** or choose **File>Close**, the SonicWALL Global VPN Client window closes but your established VPN connections remain active. A message dialog box appears notifying you that the Global VPN Client program and any enabled connections will remain active after the window is closed. If you don't want this notification message to display every time you close the Global VPN Client window, check **Don't show me this message again** and then click **OK**.


SonicWALL Global VPN Client Hide Notification
Although you have closed the connection window, the program will continue to run in the taskbar (near the clock) so that you will have your secure connections available.
12:58
Don't show me this message again
OK

You can open the SonicWALL Global VPN Client window by double-clicking the SonicWALL Global VPN Client icon in the system tray or right-clicking the icon, and selecting **Open SonicWALL Global VPN Client**.

Alert! *Exiting the SonicWALL Global VPN Client from the system tray icon menu disables any active VPN connections.*

Tip! *You can change the default launch setting for SonicWALL Global VPN Client, see "Specifying Global VPN Client Launch Options" on page 21.*

Tip! *You can create a shortcut to automatically launch the **SonicWALL Global VPN Client** window and make the VPN connection from the desktop, taskbar, or Start menu. See "Creating a VPN Policy Shortcut" on page 20.*

Tip! *You can launch the SonicWALL Global VPN Client from the command line, see "Appendix B - Running the Global VPN Client from the Command Line" on page 46.*

Making VPN Connections

Making a VPN connection from the Global VPN Client is easy because the configuration information is managed by the SonicWALL VPN gateway. The SonicWALL administrator sets the parameters for what is allowed and not allowed with the VPN connection policy. For example, for security reasons, the SonicWALL VPN Gateway administrator may not allow multiple VPN connections or the ability to access the Internet or local network while the VPN connection is enabled.

The Global VPN Client support two IPSec Keying modes: IKE using Preshared Secret and IKE using 3rd Party Certificates. Preshared Secret is the most common form of the IPSec Keying modes. If your VPN connection policy uses 3rd party certificates, you use the Certificate Manager to configure the Global VPN Client to use digital certificates.

A Pre-Shared Key (also called a Shared Secret) is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE (Internet Key Exchange) Security Association. This field can be any combination of Alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Your Pre-Shared Key is typically configured as part of your Global VPN Client provisioning. If it is not, you are prompted to enter it before you log on to the remote network.

Enabling a VPN connection with the SonicWALL Global VPN Client is a transparent two phase process. Phase 1 enables the connection, which completes the ISAKMP (Internet Security Association and Key Management Protocol) negotiation. Phase 2 is IKE (Internet Key Exchange) negotiation, which establishes the VPN connection for sending and receiving data.

When you enable a VPN connection policy, **Enabled** appears in the **Status** column of the **SonicWALL Global VPN Client** window. When phase 1 completes, **Connected** appears in the **Status** column. After phase 2 is completed, a green checkmark is displayed on the VPN connection policy icon. If an error occurs during the VPN connection, **Error** appears in the **Status** column.

Note! *If the Global VPN Client doesn't establish the VPN connection, you can use the* ***Log Viewer*** *to view the error messages to troubleshoot the problem. See "Log Viewer" on page 33.*

Enabling a VPN Connection

To establish a VPN connection using a VPN connection policy you created in the Global VPN Client, follow these instructions.

1. Enable a VPN connection policy using one of the following methods:

- If you selected **Enable this connection when the program is launched** in the **New Connection Wizard**, the VPN connection is automatically established when you launch the SonicWALL Global VPN Client.
- If your VPN connection isn't automatically established when you launch the Global VPN Client, choose one of the following methods to enable a VPN connection:

  Double-click the VPN connection policy.

  Right-click the VPN connection policy icon and select **Enable** from the menu.

  Select the VPN connection policy and press **Ctrl+B**.

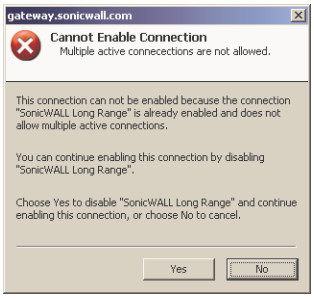
  Select the VPN connection policy, and click the **Enable** button on the toolbar

  Select the VPN connection policy, and then choose **File>Enable**.
- If the Global VPN Client icon is displayed in the system tray, right-click the icon and then select **Enable>***connection policy name*. The Global VPN Client enables the VPN connection without opening the **SonicWALL Global VPN Client** window.

2. Depending on how the VPN connection policy is configured, the **Cannot Enable Connection**, **Enter Pre-Shared Secret**, **Enter Username and Password**, and **Connection Warning** dialog boxes may be displayed, which are explained in the following sections.

Establishing Multiple Connections

You can have more than one connection enabled at a time but it depends on the connection policy parameters established at the VPN gateway. If you attempt to enable a subsequent VPN connection with a currently enabled VPN connection policy that does not allow multiple VPN connections, the **Cannot Enable Connection** message appears informing you the VPN connection cannot be made because the currently active VPN policy does not allow multiple active VPN connection. The currently enabled VPN connection policy must be disabled before enabling the new VPN connection.


gateway.sonicwall.com
Cannot Enable Connection
Multiple active connecections are not allowed.
This connection can not be enabled because the connection "SonicWALL Long Range" is already enabled and does not allow multiple active connections.
You can continue enabling this connection by disabling "SonicWALL Long Range".
Choose Yes to disable "SonicWALL Long Range" and continue enabling this connection, or choose No to cancel.
Yes
No

Entering a Pre-Shared Key

Depending on the attributes for the VPN connection policy, if no default Pre-Shared Key is used, you must have a Pre-Shared Key provided by the gateway administrator in order to make your VPN connection. If the default Pre-Shared Key is not included as part of the connection policy download or file, the **Enter Pre-Shared Key** dialog box appears to prompt you for the Pre-Shared key before establishing the VPN connection.

1. Type your Pre-Shared Key in the **Pre-shared Key** field. The Pre-Shared Key is masked for security purposes.
2. If you want to make sure you're entering the correct Pre-Shared Key, check **Don't hide the pre-shared key**. The Pre-Shared Key you enter appears unmasked in the **Pre-shared Key** field.
3. By default, the **Remember this Pre-shared Key** setting is checked allowing the Global VPN Client to save the key in an encrypted file to automatically send when enabling the VPN connection. Unchecking this setting displays the **Enter Pre-Shared Key** dialog box every time you enable the VPN connection to enter the Pre-Shared Key.
4. Click **OK**.

Username and Password Authentication

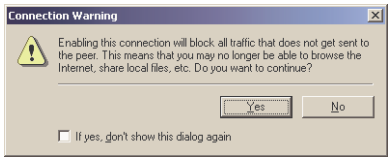
The VPN gateway typically specifies the use of XAUTH for determining GroupVPN policy membership by requiring a username and password either for authentication against the gateway's internal user database or via an external RADIUS service.

If the SonicWALL VPN gateway is provisioned to prompt you for the username and password to enter the remote network, the **Enter Username and Password** dialog box appears. Type your username and password. If permitted by the gateway, check **Remember Username and Password** to cache your username and password to automatically log in for future VPN connections. Click **OK** to continue with establishing your VPN connection.

gateway.sonicwall.com
Enter Username and Password
This peer requires that you log in with a username and password.
Please enter your username and password assigned to you by your network administrator.
Username:
Password:
The peer does not allow saving of username and password
OK
Cancel

Connection Warning

If the VPN connection policy allows only traffic to the gateway, the **Connection Warning** message appears, warning you that only network traffic destined for the remote network at the other end of the VPN tunnel is allowed. Any network traffic destined for local network interface and Internet is blocked.


Connection Warning
Enabling this connection will block all traffic that does not get sent to the peer. This means that you may no longer be able to browse the Internet, share local files, etc. Do you want to continue?
Yes
No
If yes, don't show this dialog again

You can disable the **Connection Warning** message from displaying every time you enable the VPN connection by checking **If yes, don't show this dialog box again**. Click **Yes** to continue with establishing your VPN connection.

Disabling a VPN Connection

Disabling a VPN connection terminates the VPN tunnel. You can disable a VPN connection using any of the following methods:

- Right-click the SonicWALL Global VPN Client icon on the system tray, and choose **Disable>***connection policy*.
- Right-click the VPN connection policy in the SonicWALL Global VPN Client window, and select **Disable**.
- Select the connection policy, then press **Ctrl+B**.
- Select the connection policy, and click the **Disable** button on the toolbar in the SonicWALL Global VPN Client window.

Checking the Status of a VPN Connection

The SonicWALL Global VPN Client includes a variety of indicators to determine the status of your VPN connections. The default **Details** view lists your VPN connection policies and their respective status: **Disabled**, **Enabled**, **Connected**, or **Error**.

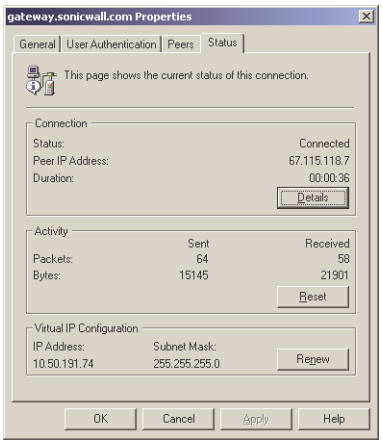
- A successfully connected VPN policy is indicated by a green check mark on the policy icon.
- A VPN policy that doesn't successfully complete all phase 2 connections displays a yellow warning on the policy icon.
- A VPN policy that cannot be successfully connected displays an error mark (red **x)** on the policy icon.
- The SonicWALL Global VPN Client icon in the system tray displays a visual indicator of data passing between the Global VPN Client and the gateway.
- The **Status** page in the **Properties** dialog box displays more detailed information about the status of an active VPN connection. To display the **Status** tab for any VPN connection, use one of the following methods:

  Double-click the active VPN connection policy.

  Select the VPN connection policy, then press **Ctrl+T**.

  Select the VPN connection policy, then click the **Status** button on the toolbar.

Right-click the VPN connection policy in the SonicWALL Global VPN Client window and select **Status**.



Tip! *For more information on the **Status** page, see .*

Creating a VPN Policy Shortcut

To streamline enabling a VPN connection, you can place a VPN connection policy on the desktop, taskbar, or Start menu. You can also place the connection policy at any other location on your system.

To create a shortcut:

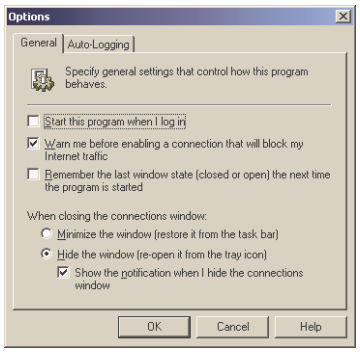
1. Select the VPN connection policy you want to create a shortcut for in the SonicWALL Global VPN Client window.
2. Choose **File>Create Shortcut** and select the shortcut option you want.

You can also right-click the VPN connection policy and then choose **Create Shortcut>***shortcut option*.

Tip! *You can also create a Desktop shortcut for the SonicWALL Global VPN Client program for easy access to all your VPN policies.*

Specifying Global VPN Client Launch Options

You can specify how the SonicWALL Global VPN Client launches and what notification windows appear using the controls in the **General** tab of the **Options** dialog box. Choose **View>Options** to display the **Options** dialog box.


Options
General
Auto-Logging
Specify general settings that control how this program behaves.
Start this program when I log in
Warn me before enabling a connection that will block my Internet traffic
Remember the last window state (closed or open) the next time the program is started
When closing the connections window:
Minimize the window (restore it from the task bar)
Hide the window (re-open it from the tray icon)
Show the notification when I hide the connections window
OK
Cancel
Help

The **General** page includes the following settings to control the launch of the Global VPN Client:

- **Start this program when I log in** - Launches the SonicWALL Global VPN Client when you log into your computer.
- **Warn me before enabling a connection that will block my Internet traffic**. Activates **Connection Warning** message notifying you that the VPN connection will block local Internet and network traffic.
- **Remember the last window state (closed or open) the next time the program is started** - Allows the Global VPN Client to remember the last window state (open or closed) the next time the program is started. For example, a user can launch the Global VPN Client from the system tray without opening a window on the desktop.
- **When closing the connections window** - Specifies how the Global VPN Client window behaves after closing. The three options include

  Minimize the window (restore it from the task bar) - Minimizes the window to taskbar and restores it from the taskbar.

  Hide the window (re-open it from the tray icon) - The default setting that hides the SonicWALL Global VPN Client window when you close it. You can open the Global VPN Client from the program icon in the system tray. Enabling this setting also displays the **Show the notification when I hide the connections window** checkbox.

  Show the notification when I hide the connections window - Checking this box activates the **SonicWALL Global VPN Client Hide Notification** window whenever you close the Global VPN Client window while the program is still running. The message tells you that the Global VPN Client program continues to run after you close (hide) the window.

SonicWALL Global VPN Client System Tray Icon

When you launch the SonicWALL Global VPN Client window, the program icon appears in the system tray on the taskbar.

This icon provides program and VPN connection status indicators as well as a menu for common SonicWALL Global VPN Client commands. Right clicking on the SonicWALL Global VPN Client icon in the system tray displays a menu of options for managing the program.

- **Open SonicWALL Global VPN Client** - Opens the program window.
- **Enable** - Displays a menu of VPN connection policies.
- **Disable** - Allows you to disable active VPN connections.
- **Open Log Viewer** - Opens the Log Viewer to view informational and error messages. See page 33 for more information on the Log Viewer.
- **Open Certificate Manager** - Opens the Certificate Manager. See “Managing Certificates” on page 32.
- **Exit** - Exits the SonicWALL Global VPN Client window and disables any active VPN connections.

Moving the mouse pointer over the SonicWALL Global VPN Client icon in the system tray displays the number of enabled VPN connections.

Managing VPN Connection Policy Properties

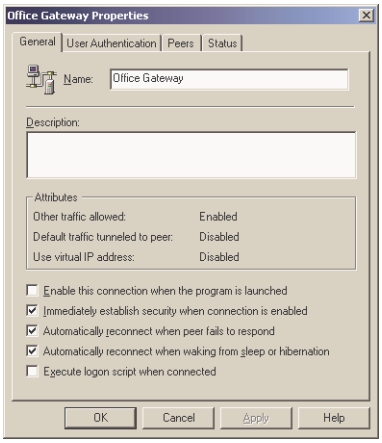
The **Connection Properties** dialog box includes the controls for configuring a specific VPN connection profile. To open the **Connection Properties** dialog box, choose one of the following methods:

- Select the connection policy and choose **File>Properties**.
- Right click the connection policy and select **Properties**.
- Select the connection policy and click the **Properties** button on the SonicWALL Global VPN Client window toolbar.

The **Connection Properties** dialog box includes the **General**, **User Authentication**, **Peers** and **Status** tabs.

General

The **General** page in the **Connection Properties** dialog box includes the following settings:



Name - Displays the name of your VPN connection policy.

Description - Displays a pop-up text about the connection policy. The text appears when your mouse pointer moves over the VPN connection policy.

Attributes - Defines the status of Tunnel All support. These settings are controlled at the SonicWALL VPN gateway.

Other traffic allowed - If enabled, your computer can access the local network or Internet connection while the VPN connection is active.

Default traffic tunneled to peer - If activated, all network traffic not routed to the SonicWALL VPN gateway is blocked. When you enable the VPN connection with this feature active, the **Connection Warning** message appears.

Use virtual IP address - Allows the VPN Client to get its IP address via DHCP through the VPN tunnel from the gateway.

Enable this connection when the program is launched - Establishes the VPN connection policy as the default VPN connection when you launch the SonicWALL Global VPN Client.

Immediately establish security when connection is enabled - Negotiates the first phase of IKE as soon as the connection is enabled instead of waiting for network traffic transmission to begin. This setting is enabled by default.

Automatically reconnect when an error occurs - With this feature is enabled, when the Global VPN Client encounters a problem connecting to the peer, it keeps retrying to make the connection. This feature allows a Global VPN Client to make a connection to a VPN connection that is temporarily disabled, without manual intervention. If the connection error is due to an incorrect configuration, such as the DNS or IP address of the peer gateway, then the connection must be manually corrected. Check the Log Viewer to determine the problem and then edit the connection. This option is enabled by default. If an error occurs with this option disabled during an attempted connection, the Global VPN Client logs the error, displays an error message dialog box, and stops the connection attempt.

Automatically reconnect when waking from sleep or hibernation - Automatically re-enables the VPN connection policy after the computer wakes from a sleep or hibernation state. This setting is disabled by default.

Execute logon script when connected - automatically execute Windows NT/2000 logon script.

Windows NT/2000 Authentication via Logon Script

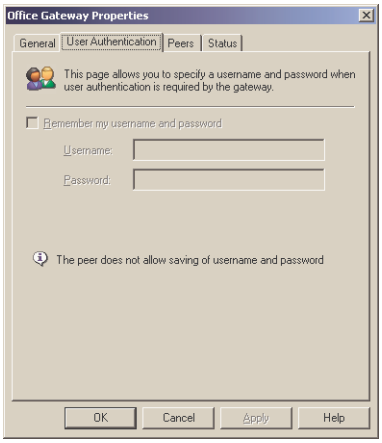
Windows NT/2000 prompts for username, password, and domain to login to the network. Windows passes the logon request to the Domain Controller (DC) for the specified domain. If the account and password are valid and security settings allow the account to log on from that computer, the DC authorizes the logon.

A logon script is a program file that runs whenever a user logs on. Each account includes profile properties that enable a user's desktop settings and other interface and operating parameters to be retained from one session to another. The profile determines the account's operating environment settings at logon. The logon script execute automatically at logon and is most often used to set environment variables, map drives, and start background processes.

The **Execute logon script** feature allows Global VPN Clients to perform domain authentication after logging into the VPN Gateway and establishing a secured tunnel. The SonicWALL passes the logon script as part of the Global VPN Client configuration to the Windows Domain Controller.

User Authentication

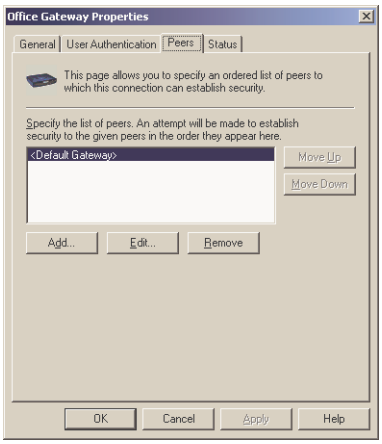
The **User Authentication** page allows you to specify a username and password when user authentication is required by the gateway. If the SonicWALL VPN gateway does not support the saving (caching) of a username and password, the settings in this page are not active and the message **The peer does not allow saving of username and password** appears at the bottom of the page.



- **Remember my username and password** - Enables the saving of your username and password for connecting to the SonicWALL VPN gateway.
- **Username** - Enter the username provided by your gateway administrator.
- **Password** - Enter the password provided by your gateway administrator.

Peers

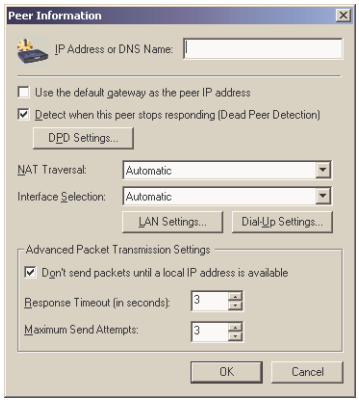
The **Peers** page allows you to specify an ordered list of VPN gateway peers that this connection policy can use (multiple entries allow a VPN connection to be established through multiple VPN gateways). An attempt is made to establish a VPN connection to the given VPN gateway peers in the order they appear in the list.



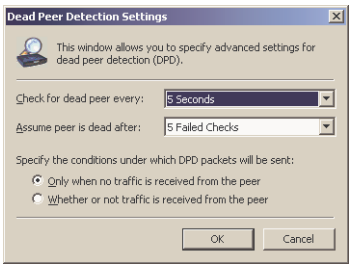
- To add a peer, click **Add**. In the **Peer Information** dialog box, enter the IP address or DNS Name in the **IP Address or DNS Name** box, then click **OK**.
- To edit a peer entry, select the peer name and click **Edit**. In the **Peer Information** dialog box, make your changes, then click **OK**.
- To delete a peer entry, select the peer entry and click **Remove**.

Peer Information Dialog Box

The **Peer Information** dialog box allows you to add or edit peer information.



- **IP Address or DNS Name** - Specifies the peer VPN gateway IP address or DNS name.
- **Use the default gateway as the peer IP address** - Specifies the default gateway as the peer IP address.
- **Detect when this peer stops responding** - Automatically initiates VPN connection again if the VPN gateway does not respond for four consecutive heart beats. The Global VPN Client exchanges “heart beat” packets to detect if the peer gateway is alive. This setting is enabled by default.
- **DPD Settings** - Displays the **Dead Peer Detection** Settings dialog box.


Dead Peer Detection Settings
This window allows you to specify advanced settings for dead peer detection (DPD).
Check for dead peer every:
5 Seconds
Assume peer is dead after:
5 Failed Checks
Specify the conditions under which DPD packets will be sent:
Only when no traffic is received from the peer
Whether or not traffic is received from the peer
OK
Cancel

Check for dead peer every - choose from 5, 10, 15, 20, 25, or 30 seconds.

Assume peer is dead after - choose from 3, 4, or 5 Failed Checks.

Specify the conditions under which DPD packets will be sent - Choose either **Only when no traffic is received from the peer** or **whether or not traffic is received from the peer**.

- **NAT Traversal** - Choose one of the following three menu options:

  Automatic - Automatically determines whether NAT traversal is forced on or disabled.

  Forced On - Forces the use of UDP encapsulation of IPSec packets even when there is no NAPT/NAT device in between the peers.

  Disabled - Disables use of UDP encapsulation of IPSec packets between the peers.

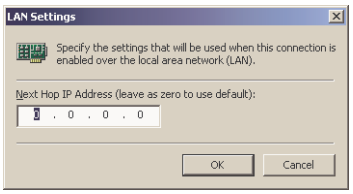
- **Interface Selection** - Defines the interface used by this VPN connection policy.

  Automatic - Automatically determines the availability of each interface beginning with the LAN interface. If the LAN interface is not available, the Global VPN Client uses the Dial-Up interface.

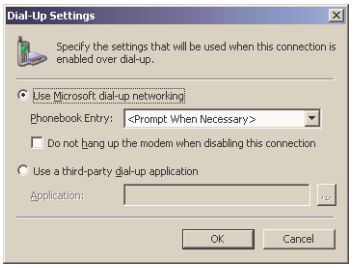
  LAN Only - Defaults to the LAN interface only.

  Dial-Up Only - Defaults to the Dial-Up interface only.

- **LAN Settings** - Displays **LAN Settings** dialog box for specifying the setting used when this connection is enabled over the LAN. Type the IP address in the **Next Hop IP Address** field to specify the IP address of a different route than the default route. Leaving the setting as zeros instructs the Global VPN Client to use the default route.


LAN Settings
Specify the settings that will be used when this connection is enabled over the local area network (LAN).
Next Hop IP Address (leave as zero to use default):
0 . 0 . 0 . 0
OK
Cancel

- **Dial-Up Settings** - Displays the **Dial-Up Settings** dialog box, which allows you to select the dial-up profile to use making a dial-up VPN connection.


Dial-Up Settings
Specify the settings that will be used when this connection is enabled over dial-up.
Use Microsoft dial-up networking
Phonebook Entry:
<Prompt When Necessary>
Do not hang up the modem when disabling this connection
Use a third-party dial-up application
Application:
OK
Cancel

  Use Microsoft dial-up networking - Uses the Microsoft dial-up networking profile you specify for making the VPN connection. Select the Dial-up networking profile from the **Phonebook Entry** list. Check the **Do not hang up the modem when disabling this connection** to keep the dial-up network connection active after disabling the VPN connection.

  Use a third-party dial-up application - Select this option to use a third party dial-up program. Type the path in the **Application** field or use the browse **...** button to locate the program.

- **Advanced Packet Transmission Settings** - Allows manual configuration of the timeout value and retries for IKE negotiations.

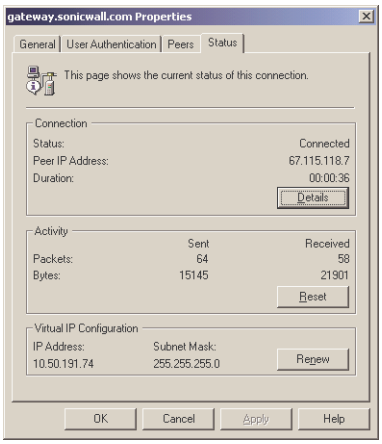
  Don’t send packets until a local IP address is available - Delays sending packets until a local IP address becomes available.

  Response Timeout (in seconds) - Specifies a timeout value for the VPN connection attempt.

  Maximum Send Attempts - Specifies the number of IKE negotiation retries.

Status

The **Status** page shows the current status of the connection.



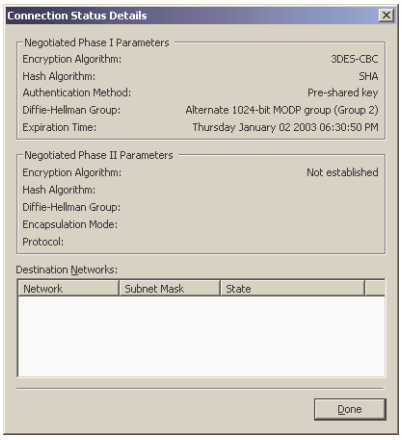
- **Connection**

  Status - Indicates whether VPN connection policy is enabled or disabled.

  Peer IP Address - Displays the IP address of the VPN connection peer.

  Duration - Displays connection time.

  Details - Displays the **Connection Status Details** dialog box, which specifies the negotiated phase 1 and phase 2 parameters as well as the status of all individual phase 2 SAs.



- **Activity**

  Packets - Displays number of packets sent and received through VPN tunnel.

  Bytes - Displays number of bytes sent and received through VPN tunnel.

  Reset - Resets the status information.

- **Virtual IP Configuration**

  IP Address - The IP address assigned via DHCP through the VPN tunnel from the VPN gateway.

  Subnet Mask - The subnet assigned via DHCP through the VPN tunnel from the VPN gateway.

  Renew - Renews DHCP lease information.

Managing VPN Connection Policies

The SonicWALL Global VPN Client supports as many VPN connection policies as you need. To help you manage these connection policies, the Global VPN Client provides the following connection policy management tools.

Displaying Connection Policies

You can display VPN connection policy icons using standard Windows icon display modes by choosing **Large Icons**, **Small Icons**, **List**, or **Details** from the **View** menu in the SonicWALL Global VPN Client window.

The default **Details** view provides a handy view of your VPN connection profiles including their gateway IP addresses or FQDNs as well as the status of the connection policies (**Disabled**, **Enabled**, **Connected**, or **Error**).

Arranging Connection Policies

Over time, as the number of VPN connection policies can increase in the SonicWALL Global VPN Client window, you may want to arrange them for quicker access. You can arrange your VPN connection policies in the SonicWALL Global VPN Client window by choosing **View>Arrange Icons by**. You can arrange VPN connection profiles by:

Name - Sorts connection policies by name.

Peer - Sorts connection policies by gateway IP address.

Status - Sorts connection policies by connection status.

Ascending - Sorts Name, Gateway, or Status arrangements in ascending order. If unchecked, policy arrangements are sorted in descending order.

The default arrangement is by **Name** in **Ascending** order**.**

Renaming a Connection Policy

To rename a connection policy, select the policy and click on the **Rename** button on the toolbar or choose **File>Rename**, then type in the new name. You can also right-click the connection policy and choose **Rename** from the menu.

Deleting a Connection Policy

To delete a connection policy, select the policy, press **Del** or choose **File>Delete**. You can also right-click the policy name and choose **Delete**. You cannot delete an active VPN connection. Disable the VPN connection, then delete it.

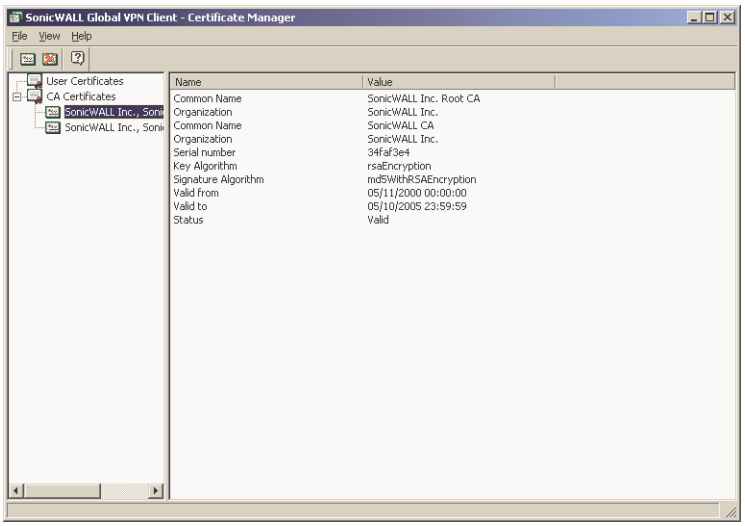
Selecting All Connection Policies

Choosing **View>Select All** or pressing **Ctrl+A** selects all the connection policies in the SonicWALL Global VPN Client window.

Managing Certificates

The **Certificate Manager** allows you to manage digital certificates used by the SonicWALL Global VPN Client for VPN connections. If your VPN gateway uses digital certificates, you must import the CA and Local Certificates into the **Certificate Manager**.

To open the Certificate Manager, click the **Certificate Manager** button on the SonicWALL Global VPN Client window toolbar, choose **View>Certificate Manager**, or press **Ctrl+M**.



The left pane of the **Certificate Manager** window lists the active Local and CA certificates currently used by your VPN policies. User Certificates list the local digital certificates used to establish the VPN Security Association. CA Certificates list the digital certificates used to validate the user certificates.

- Click on the certificate in the left pane to display the certificate information in the right pane.
- Click the **Import** button on the toolbar, press **Ctrl+I**, or choose **File>Import Certificate** from the to display the **Import Certificate** window to import a certificate file.
- Click the **Delete** button on the toolbar, press **Del**, or choose **File>Delete Certificate** to delete the selected certificate.
- Choose **View>Toolbar** to hide the toolbar.
- Choose **View>Status Bar** to hide the status bar.

Tip! *For more information on using certificates for your VPN on the SonicWALL, see the SonicWALL Administrator's Guide for your SonicWALL.*

Troubleshooting SonicWALL Global VPN Client

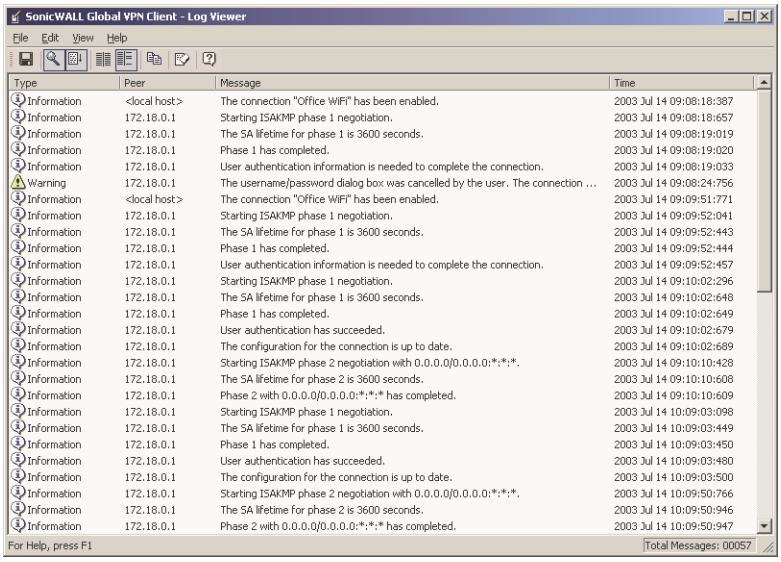
The SonicWALL Global VPN Client provides tools for troubleshooting your VPN connections. This section explains using Log Viewer, generating a Help Report, accessing SonicWALL's Support site, using SonicWALL Global VPN Client help system, and uninstalling the Global VPN Client.

Log Viewer

The **SonicWALL Global VPN Client Log Viewer** window displays messages about Global VPN Client activities. The Log Viewer window displays the type of message (**Information**, **Error**, or **Warning**) the peer IP address or FQDN, and the date and time the message was generated.

Tip! *See **Appendix D** for complete listing of Log Viewer messages.*

To open the **Log Viewer** window, click the **Log Viewer** button on the Global VPN Client window toolbar, or choose **View>Log Viewer**, or press **Ctrl+L**.

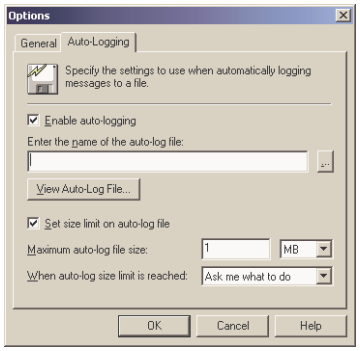

SonicWALL Global VPN Client - Log Viewer
File Edit View Help
Type Peer Message Time
Information <local host> The connection "Office WiFi" has been enabled. 2003 Jul 14 09:08:18:387
Information 172.18.0.1 Starting ISAKMP phase 1 negotiation. 2003 Jul 14 09:08:18:657
Information 172.18.0.1 The SA lifetime for phase 1 is 3600 seconds. 2003 Jul 14 09:08:19:019
Information 172.18.0.1 Phase 1 has completed. 2003 Jul 14 09:08:19:020
Information 172.18.0.1 User authentication information is needed to complete the connection. 2003 Jul 14 09:08:19:033
Warning 172.18.0.1 The username/password dialog box was cancelled by the user. The connection ... 2003 Jul 14 09:08:24:756
Information <local host> The connection "Office WiFi" has been enabled. 2003 Jul 14 09:09:51:771
Information 172.18.0.1 Starting ISAKMP phase 1 negotiation. 2003 Jul 14 09:09:52:041
Information 172.18.0.1 The SA lifetime for phase 1 is 3600 seconds. 2003 Jul 14 09:09:52:443
Information 172.18.0.1 Phase 1 has completed. 2003 Jul 14 09:09:52:444
Information 172.18.0.1 User authentication information is needed to complete the connection. 2003 Jul 14 09:09:52:457
Information 172.18.0.1 Starting ISAKMP phase 1 negotiation. 2003 Jul 14 09:10:02:296
Information 172.18.0.1 The SA lifetime for phase 1 is 3600 seconds. 2003 Jul 14 09:10:02:648
Information 172.18.0.1 Phase 1 has completed. 2003 Jul 14 09:10:02:649
Information 172.18.0.1 User authentication has succeeded. 2003 Jul 14 09:10:02:679
Information 172.18.0.1 The configuration for the connection is up to date. 2003 Jul 14 09:10:02:689
Information 172.18.0.1 Starting ISAKMP phase 2 negotiation with 0.0.0.0/0.0.0.0:*:*:*. 2003 Jul 14 09:10:10:428
Information 172.18.0.1 The SA lifetime for phase 2 is 3600 seconds. 2003 Jul 14 09:10:10:608
Information 172.18.0.1 Phase 2 with 0.0.0.0/0.0.0.0:*:*:* has completed. 2003 Jul 14 09:10:10:609
Information 172.18.0.1 Starting ISAKMP phase 1 negotiation. 2003 Jul 14 10:09:03:098
Information 172.18.0.1 The SA lifetime for phase 1 is 3600 seconds. 2003 Jul 14 10:09:03:449
Information 172.18.0.1 Phase 1 has completed. 2003 Jul 14 10:09:03:450
Information 172.18.0.1 User authentication has succeeded. 2003 Jul 14 10:09:03:480
Information 172.18.0.1 The configuration for the connection is up to date. 2003 Jul 14 10:09:03:500
Information 172.18.0.1 Starting ISAKMP phase 2 negotiation with 0.0.0.0/0.0.0.0:*:*:*. 2003 Jul 14 10:09:50:766
Information 172.18.0.1 The SA lifetime for phase 2 is 3600 seconds. 2003 Jul 14 10:09:50:946
Information 172.18.0.1 Phase 2 with 0.0.0.0/0.0.0.0:*:*:* has completed. 2003 Jul 14 10:09:50:947
For Help, press F1
Total Messages: 00057

The Log Viewer provides the following features to help you manage log messages:

- To save a current log to a **.txt** file, click the **Save** button on the toolbar, press **Ctrl+S**, or choose **File>Save**.
- To enable or disable message capturing, click the **Capture** button on the toolbar, press **Ctrl+M**, or choose **View>Stop Capturing Messages** or **View>Start Capturing Messages**.
- To start or stop automatic scrolling of messages to the latest message, click the **Auto Scroll** button on the toolbar, press **Ctrl+T**, or choose **View>Start Auto Scroll** or **View>Stop Auto Scroll**.
- To select all messages, press **Ctrl+A** or choose **Edit>Select All**.
- To copy log contents for pasting into another application, select the messages you want to copy, then click the **Copy** button on the toolbar, press **Ctrl+C**, or choose **Edit>Copy**.
- To clear current log information, click the **Clear** button on the toolbar, press **Crtl+X**, or choose **Edit>Clear**.
- To specify the message display level from **All Messages** to **Filtered Messages**, click the **Filtered Messages** button on the toolbar. You can also choose **View>All Messages** or **View>All Messages**.
- To remove redundant messages from displaying, choose **View>Ignore Redundant Messages** or press **Ctrl+I**.
- To hide the toolbar in the **Log Viewer** window, choose **View>Toolbar**.
- To hide the status bar in the **Log Viewer** window, choose **View>Status Bar**.

Setting Up Log Files

The **Auto-Logging** tab in the **Options** dialog box specifies the settings to use when automatically logging messages to a file. Log files are saved as text files (**.txt**). To access Auto-Logging from the SonicWALL Global VPN Client window, choose **View>Options**, then click the **Auto-Logging** tab.



Enable auto-logging - Enables auto-logging to a file.

Enter the name of the auto-log file - Specifies the file to save the logging messages. Clicking on the **...** button allows you to specify the location of your auto-log file.

Set size limit on auto-log file - Activates a maximum size limit for the log file.

Maximum auto-log file size - Specifies the maximum file size in KB or MB.

When auto-log size limit is reached - Instructs Auto-logging what to do when log file size is reached.

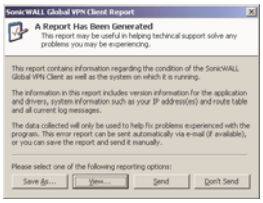
Ask me what to do - Prompts you when the log file reaches maximum size to choose either **Stop auto-logging** or **Overwrite auto-log file**.

Stop auto-logging - Stops auto-logging when maximum file size is reached.

Overwrite auto-log file - Overwrites existing auto-log file after maximum file size is reached.

Generating a Help Report

Choosing **Help>Generate Report** in the SonicWALL Global VPN Client window displays the **SonicWALL Global VPN Client Report** dialog box.

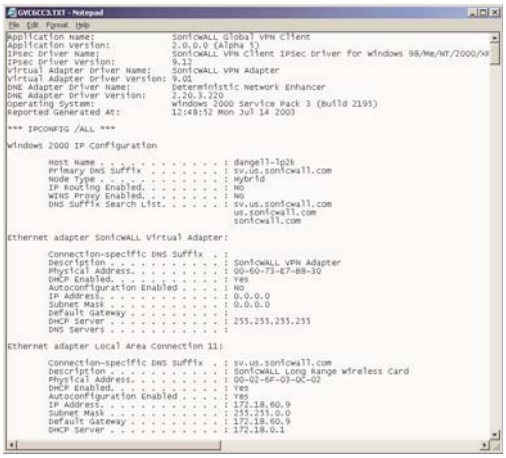

SonicWALL Global VPN Client Report
A Report Has Been Generated
This report may be useful in helping technical support solve any problems you may be experiencing.
This report contains information regarding the condition of the SonicWALL Global VPN Client as well as the system on which it is running.
The information in this report includes version information for the application and drivers, system information such as your IP address(es) and route table and all current log messages.
The data collected will only be used to help fix problems experienced with the program. This error report can be sent automatically via e-mail (if available), or you can save the report and send it manually.
Please select one of the following reporting options:
Save As...
View...
Send
Don't Send

Generate Report creates a report containing useful information for getting help in solving any problems you may be experiencing. The report contains information regarding the condition of the SonicWALL Global VPN Client as well as the system it's running on.

Information in this report includes:

- Version information
- Drivers
- System information
- IP addresses
- route table
- Current log messages.

To view the report in the default text editor window, click **View**.


GVC6CC3.TXT - Notepad
File Edit Format Help
Application Name: SonicWALL Global VPN Client
Application Version: 2.0.0.0 (Alpha 5)
IPSec Driver Name: SonicWALL VPN Client IPSec Driver for Windows 98/Me/NT/2000/XP
IPSec Driver Version: 9.12
Virtual Adapter Driver Name: SonicWALL VPN Adapter
Virtual Adapter Driver Version: 9.01
DNE Adapter Driver Name: Deterministic Network Enhancer
DNE Adapter Driver Version: 2.20.3.220
Operating System: Windows 2000 Service Pack 3 (Build 2195)
Reported Generated At: 12:48:52 Mon Jul 14 2003
*** IPCONFIG /ALL ***
Windows 2000 IP Configuration
Host Name . . . . . : dangell-1g2k
Primary DNS Suffix . . . . . : sv.us.sonicwall.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : sv.us.sonicwall.com
us.sonicwall.com
sonicwall.com
Ethernet adapter SonicWALL Virtual Adapter:
Connection-specific DNS Suffix . :
Description . . . . . : SonicWALL VPN Adapter
Physical Address. . . . . : 00-60-73-E7-B8-30
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : No
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
DHCP Server . . . . . : 255.255.255.255
DNS Servers . . . . . :
Ethernet adapter Local Area Connection 11:
Connection-specific DNS Suffix . : sv.us.sonicwall.com
Description . . . . . : SonicWALL Long Range Wireless Card
Physical Address. . . . . : 00-02-6F-03-0C-02
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 172.18.60.9
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.18.60.9
DHCP Server . . . . . : 172.18.0.1

To save the report to a text file, click **Save As**.

To send the report via e-mail, click **Send**.

To close the report window without taking any action, click **Don't Send**.

Technical Support

Selecting **Help**>**Technical Support** accesses the SonicWALL Support site (www.sonicwall.com/support). The SonicWALL Support site offer a full range of support services including extensive online resources and information on SonicWALL's enhanced support programs.

Help Topics

Selecting **Help**>**Help Topics** displays SonicWALL Global VPN Client help system window. You can access help topics using the following options:

- **Contents** - displays help in a table of contents view.
- **Index** - displays help in an alphabetical topic view.
- **Search** - allows you to search the help system using keywords.

Uninstalling the SonicWALL Global VPN Client

You can easily uninstall the SonicWALL Global VPN Client and choose to save or delete your VPN connection policies as part of the uninstall process. To uninstall the SonicWALL Global VPN Client:

Alert! *You must exit the SonicWALL Global VPN Client before uninstalling the program.*

1. Launch the Windows Control Panel
2. Double-click **Add/Remove Programs**
3. Select SonicWALL Global VPN Client and then click **Change/Remove**. The SonicWALL Global VPN Client Setup Wizard appears.
4. In the **Confirm File Deletion dialog box,** click **OK** to confirm the removal of the SonicWALL Global VPN Client.
5. Select **Delete all individual user profiles** if you want to delete all your existing VPN connection profiles. If you leave this setting unchecked, the VPN connection profiles are saved and appear again when you install the SonicWALL Global VPN Client at another time.
6. Select **Retain MAC Address** if you want to retain the same SonicWALL VPN Adapter MAC address the next time you install the Global VPN Client. Click **Next**.
7. After the Global VPN Client is removed, select **Yes, I want to restart my computer now**, and then click **Finish**.

SONICWALL GLOBAL VPN CLIENT SOFTWARE LICENSE AGREEMENT

This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this SLA. If you do not agree to the terms of this SLA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

- The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as by other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
- Title to the SOFTWARE PRODUCT licensed to you and all copies thereof are retained by SonicWALL or third parties from whom SonicWALL has obtained a licensing right. You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This SLA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this SLA.
- The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.
- You may install and use one copy of the SOFTWARE PRODUCT, or any prior version for the same operating system, on a single computer.
- You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network. However, you must acquire and dedicate a license for each separate computer on which the SOFTWARE PRODUCT is installed or run from the storage device. A license for the SOFTWARE PRODUCT may not be shared or used concurrently on different computers.
- You may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.
- You may not rent, lease, or lend the SOFTWARE PRODUCT.
- You may permanently transfer all of your rights under this SLA, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, and this SLA); the recipient agrees to the terms of this SLA; and you obtain prior written consent from SonicWALL. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT.

- The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this SLA.

LICENSE

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for SonicWALL

Internet Security Appliances.

OEM - If the SOFTWARE PRODUCT is modified and enhanced for a SonicWALL OEM partner, you must adhere to the software license agreement of the SonicWALL OEM partner.

EXPORTS LICENSE

Licensee will comply with, and will, at SonicWALL's request, demonstrate such compliance with all applicable export laws, restrictions, and regulations of the U.S. Department of Commerce, the U.S. Department of Treasury and any other any U.S. or foreign agency or authority. Licensee will not export or re-export, or allow the export or re-export of any product, technology or information it obtains or learns pursuant to this Agreement (or any direct product thereof) in violation of any such law, restriction or regulation, including, without limitation, export or re-export to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country subject to applicable U.S. trade embargoes or restrictions, or to any party on the U.S. Export Administration Table of Denial Orders or the U.S. Department of Treasury List of Specially Designated Nationals, or to any other prohibited destination or person pursuant to U.S. law, regulations or other provisions.

SUPPORT SERVICES

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in "online" documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this SLA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

UPGRADES

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this SLA. If the

SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

COPYRIGHT

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by SonicWALL or its suppliers/licensors. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

U.S. GOVERNMENT RESTRICTED RIGHTS

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense ("DOD"), the Software is subject to "Restricted Rights", as that term is defined in the DOD Supplement to the Federal Acquisition Regulations ("DFAR") in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations ("FAR"). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

MISCELLANEOUS

This SLA represents the entire agreement concerning the subject matter hereof between the parties and supercedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This SLA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this SLA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

TERMINATION

This SLA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this SLA if you fail to comply with the terms and conditions of this SLA. In such event, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

LIMITED WARRANTY

SonicWALL warrants that a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and b) any Support Services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the SOFTWARE PRODUCT are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES

SonicWALL's and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

NO OTHER WARRANTIES

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide Support Services. This Limited Warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

LIMITATION OF LIABILITY

To the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any damages (including without limitation special, incidental, indirect, or consequential) whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide Support Services, even if SonicWALL has been advised of the possibility of such damages. In any case, SonicWALL's entire liability under any provision of this SLA shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S. $10.00; provided, however, if you have entered into a SonicWALL Support Services Agreement, SonicWALL's entire liability regarding Support Services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

SonicWALL Global VPN Client Support

SonicWALL's comprehensive support services protect your network security investment and offer the support you need - when you need it. SonicWALL Global VPN Client support is included as part of the support program of your SonicWALL Internet Security Appliance.

For more information on SonicWALL Support Services, please visit www.sonicwall.com/products/supportservices.htm

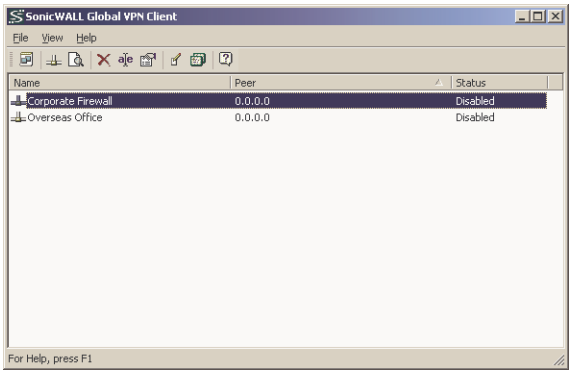
You can purchase/activate SonicWALL Support Services through your mySonicWALL.com account at www.mysonicwall.com.

For Web based technical support, please visit www.sonicwall.com/support.

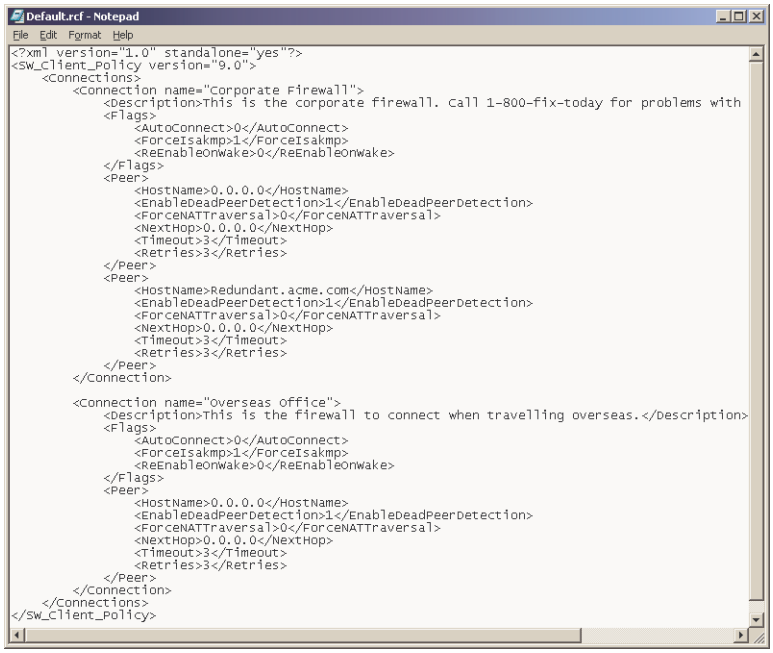
Appendix A: Using the default.rcf File

The **default.rcf** file allows the SonicWALL VPN Gateway administrator to create and distribute preconfigured VPN connections for SonicWALL Global VPN Clients. The SonicWALL VPN Gateway administrator can distribute the **default.rcf** file with the Global VPN Client software to automatically create preconfigured VPN connections for streamlined deployment.

The VPN connections created from the **default.rcf file** appear in the SonicWALL Global VPN Client window. The Global VPN Client user simply enables the VPN connection and after XAUTH authentication with a username and password, the policy download is automatically completed.



The default.rcf file includes preconfigured VPN connection settings. You can view the contents of the **default.rcf** file using any text editor, such as Windows Notepad.



How the Global VPN Client uses the default.rcf File

When the Global VPN Client starts up, the program always looks for the **SonicWALL Global VPN Client.rcf** file in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory. If this file does not exist the Global VPN Client looks for the default.rcf file in the *C:\Program Files\SonicWALL\SonicWALL Global VPN Client* directory.

The Global VPN Client reads the **default.rcf** file, if it exists and creates the **SonicWALL Global VPN Client.rcf** file in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory. The encrypted **SonicWALL Global VPN Client.rcf** file contains all the VPN connection configuration information for the SonicWALL Global VPN Client.

Installing the default.rcf File

There are three ways you can install the **default.rcf** file for your SonicWALL Global VPN Client.

Include the default.rcf File with the Global VPN Client Software

If the **default.rcf** file is included with your SonicWALL Global VPN Client software, when you install the Global VPN Client program, the **SonicWALL Global VPN Client.rcf** file is automatically created in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory based on the settings defined in the **default.rcf** file. The VPN connections appear in the **SonicWALL Global VPN Client** window.

Tip! *You can verify the default.rcf file is included with your SonicWALL Global VPN Client software by looking for the default.rcf file in the directory with the program files.*

Alert! *The **default.rcf** file must be included in the default Global VPN Client installation directory C:\Program Files\SonicWALL\SonicWALL Global VPN Client\ for the program to write the SonicWALL Global VPN Client.rcf file based on the settings defined in the default.rcf file.*

Add the default.rcf file to the Default Global VPN Client Directory

If the Global VPN Client software is already installed and you have not created any VPN connections, you can add the **default.rcf** file to the default Global VPN Client installation directory *C:\Program Files\SonicWALL\SonicWALL Global VPN Client*\. When you launch the Global VPN Client, the **SonicWALL Global VPN Client.rcf** file is created in the *C:\Documents and Settings**<user>**Application Data**SonicWALL**SonicWALL Global VPN Client*\ directory based on the default.rcf file settings.

Replace the Existing SonicWALL Global VPN Client.rcf File

If the Global VPN Client is installed with VPN connections, you can remove the **SonicWALL Global VPN Client.rcf** file from the *C:\Documents and Settings**<user>**Application Data**SonicWALL**SonicWALL Global VPN Client*\ directory and add the **default.rcf** file to the default Global VPN Client installation directory *C:\Program Files**SonicWALL**SonicWALL Global VPN Client*\. When your launch the Global VPN Client, the SonicWALL Global VPN Client.rcf file is created in the *C:\Documents and Settings**<user>**Application Data**SonicWALL**SonicWALL Global VPN Client*\ directory based on the **default.rcf** file settings.

Alert! *You cannot copy the **SonicWALL Global VPN Client.rcf** file created from the settings defined in the **default.rcf** file for one Global VPN Client to replace an existing **SonicWALL Global VPN Client.rcf** file of another Global VPN Client.*

Alert! *Removing an existing **SonicWALL Global VPN Client.rcf** file will remove the VPN connections created in the Global VPN Client. These VPN connections can be added again from the Global VPN Client into the new **SonicWALL Global VPN Client.rcf** file.*

Troubleshooting

If there are any incorrect entries or typos in your **default.rcf** file, the settings in the **default.rcf** file will not be incorporated into the Global VPN Client and no connection profiles will appear in the Global VPN Client window. An error message ***Failed to parse*** configuration file appears in the Global VPN Client Log Viewer.

The SonicWALL Global VPN Client.rcf file created by the default.rcf file must be deleted from the *C:\Documents and Settings**<user>**Application Data**SonicWALL**SonicWALL Global VPN Client*\ directory and the default.rcf file edited to correct the errors.

Note! *See the SonicWALL Global VPN Client Administrator's Guide for more information on creating and editing the **default.rcf** file.*

Appendix B - Running the Global VPN Client from the Command Line

The SonicWALL Global VPN Client can run from the command line in Microsoft Windows.

To start the Global VPN Client from the command prompt, navigate to the directory containing the SWGVpnClient .exe file, enter **SWGVpnClient .exe** and press **Enter**.

You can use the following options to perform a variety of Global VPN Client actions from the command line.

- **/E "*Connection Name*"** Enables the specific connection.
- **/D "*Connection Name*"** Disables the specific connection.
- **/Q** - Quits a running an instance of the program. Ignored if program is not already running.
- **/A [*filename*]** - Starts the program and sends all messages to the specified log file. If no log file is specified, the default file name is **gvcauto.log**. If the program is already running, this option is ignored.
- **/U "Username"** - Username to pass to XAUTH. Must be used in conjunction with **/E**.
- **/P "Password"** - Password to pass to XAUTH. Must be used in conjunction with **/E**.

SonicWALL,Inc.
1143 Borregas Avenue
Sunnyvale,CA 94089-1306
T: 408.745.9600
F: 408.745.9300
www.sonicwall.com

© 2003 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and / or registered trademarks of their respective companies. Specifications and descriptions subject to change with out notice.

P/ N 232- 000333- 01
Rev A 10 / 03